

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-66706

(43) 公開日 平成11年(1999) 3月9日

(51) Int.Cl. <sup>6</sup>	識別記号	F I		
G 1 1 B 19/04	5 0 1	G 1 1 B 19/04	5 0 1 H	
7/00		7/00	Q	
20/10		20/10	D	
			F	
20/14	3 4 1	20/14	3 4 1 A	
審査請求 未請求 請求項の数20 O L (全 16 頁) 最終頁に続く				

(21) 出願番号 特願平9-228234

(22) 出願日 平成9年(1997) 8月25日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 志村 成生

神奈川県川崎市幸区柳町70番地 株式会社

東芝柳町工場内

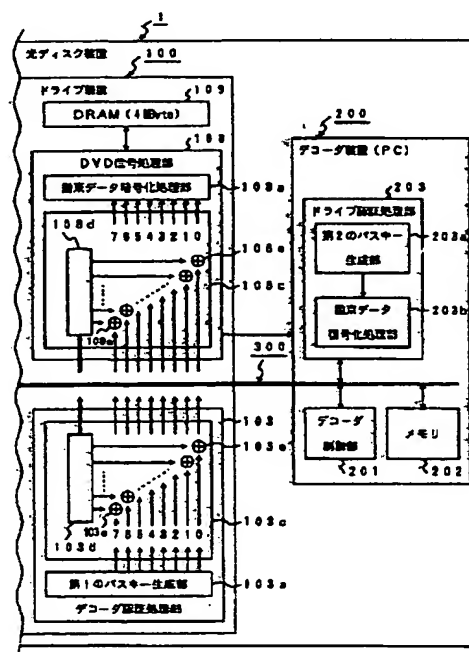
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 光ディスク再生装置及び光ディスク記録再生装置

(57) 【要約】

【課題】 光ディスクデータの不正コピーを防止することが可能な光ディスク再生装置及び光ディスク記録再生装置を提供すること。

【解決手段】 光ディスクから光ディスクデータを読み出し提供するドライブ装置(100)と、光ディスクデータを再生するデコーダ装置(200)と、各装置間及び各装置内のデータ通信を担う通信手段(300)とを備えた光ディスク装置(1)において、光ディスクデータを暗号化する第1のデータを生成し提供するデータ生成手段(103a)と、第1のデータを暗号化して第2のデータを生成し、この第2のデータを前記通信手段を介して送信する暗号化手段(103c)と、通信手段を介して第2のデータを受信し、この第2のデータを復号化して第1のデータを生成する復号化手段(108c)とを備えている。



## 【特許請求の範囲】

【請求項1】光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、

前記光ディスクデータを暗号化するための暗号化用データを生成し提供する暗号化用データ生成手段と、  
前記通信手段と所定の状態で接続されたものであって、前記暗号化用データを前記通信手段へ出力する出力手段と、

前記通信手段と前記所定の状態と同一の状態で接続されたものであって、前記通信手段を介して前記暗号化用データを入力する入力手段と、

を備えたことを特徴とする光ディスク再生装置。

【請求項2】光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、

前記ドライブ装置側に設けられたものであって、前記光ディスクデータを暗号化するための第1の暗号化用データを生成し提供する第1の暗号化用データ生成手段と、

前記ドライブ装置側に設けられ、且つ前記通信手段と所定の状態で接続されたものであって、前記第1の暗号化用データを前記通信手段へ出力する出力手段と、

前記ドライブ装置側に設けられ、且つ前記通信手段と前記所定の状態と同一の状態で接続されたものであって、前記通信手段を介して前記第1の暗号化用データを入力する入力手段と、

前記ドライブ装置側に設けられたものであって、前記入力手段から入力された前記第1の暗号化用データにより第1の光ディスクデータに対して暗号化処理を施し、この第1の光ディスクデータから第2の光ディスクデータを生成し、この第2の光ディスクデータを前記通信手段を介して前記デコーダ装置側へ提供する暗号化処理手段と、

前記デコーダ装置側に設けられたものであって、前記光ディスクデータを暗号化するための前記第1の暗号化用データと同一の第2の暗号化用データを生成し提供する第2の暗号化用データ生成手段と、

前記デコーダ装置側に設けられたものであって、前記通信手段を介して前記第2の光ディスクデータを受取り、前記第2の暗号化用データによりこの第2の光ディスク

データに対して復号化処理を施し、この第2の光ディスクデータから前記第1の光ディスクデータを生成し提供する復号化処理手段と、

を備えたことを特徴とする光ディスク再生装置。

【請求項3】光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、

前記光ディスクデータを暗号化するための第1の暗号化用データを生成し提供する第1の暗号化用データ生成手段と、

前記第1の暗号化用データに対して暗号化処理を施し、この第1の暗号化用データから第2の暗号化用データを生成し、この第2の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、

前記通信手段を介して前記第2の暗号化用データを受信し、この第2の暗号化用データに対して復号化処理を施し、この第2の暗号化用データから前記第1の暗号化用データを生成し提供する復号化処理手段と、

を備えたことを特徴とする光ディスク再生装置。

【請求項4】光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、

前記ドライブ装置側に設けられたものであって、前記光ディスクデータを暗号化するための第1の暗号化用データを生成し提供する第1の暗号化用データ生成手段と、

前記ドライブ装置側に設けられたものであって、前記第1の暗号化用データに対して暗号化処理を施し、この第1の暗号化用データから第2の暗号化用データを生成し、この第2の暗号化用データを前記通信手段を介して送信する第1の暗号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記通信手段を介して前記第2の暗号化用データを受信し、この第2の暗号化用データに対して復号化処理を施し、この第2の暗号化用データから前記第1の暗号化用データを生成し提供する第1の復号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記第1の復号化処理手段により生成された前記第1の暗号化用データにより第1の光ディスクデータに対して暗号化処理を施し、この第1の光ディスクデータから第2の光ディスクデータを生成し、この第2の光ディスクデータ

を前記通信手段を介して前記デコーダ装置側へ提供する第2の暗号化処理手段と、

前記デコーダ装置側に設けられたものであって、前記光ディスクデータを暗号化するための前記第1の暗号化用データと同一の第3の暗号化用データを生成し提供する第3の暗号化用データ生成手段と、

前記デコーダ装置側に設けられたものであって、前記通信手段を介して前記第2の光ディスクデータを受取り、前記第3の暗号化用データによりこの第2の光ディスクデータに対して復号化処理を施し、この第2の光ディスクデータから前記第1の光ディスクデータを生成し提供する第2の復号化処理手段と、

を備えたことを特徴とする光ディスク再生装置。

【請求項5】光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、

前記光ディスクデータを暗号化するための第1の暗号化用データを生成し提供する第1の暗号化用データ生成手段と、

前記第1の暗号化用データを暗号化するための第2の暗号化用データを生成し提供する第2の暗号化用データ生成手段と、

前記第2の暗号化データにより前記第1の暗号化用データに対して暗号化処理を施し、前記第1の暗号化用データから第3の暗号化用データを生成し、この第3の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、

前記通信手段を介して前記第2及び第3の暗号化用データを受信し、この第2の暗号化用データによりこの第3の暗号化用データに対して復号化処理を施し、この第3の暗号化用データから第1の暗号化用データを生成し提供する復号化処理手段と、

を備えたことを特徴とする光ディスク再生装置。

【請求項6】前記暗号化処理手段が、前記第1の暗号化用データと前記第2の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第3の暗号化用データとして提供する第1の排他的論理和算出手段を有し、

前記復号化処理手段が、前記第2の暗号化用データと前記第3の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第1の暗号化用データとして提供する第2の排他的論理和算出手段を有する、ことを特徴とする請求項5に記載の光ディスク再生装置。

【請求項7】光ディスクに対して光ビームを照射し、光

ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、

前記ドライブ装置側に設けられたものであって、前記光ディスクデータを暗号化するための第1の暗号化用データを生成し提供する第1の暗号化用データ生成手段と、前記ドライブ装置側に設けられたものであって、前記第1の暗号化用データを暗号化するための第2の暗号化用データを生成し提供する第2の暗号化用データ生成手段と、

前記ドライブ装置側に設けられたものであって、前記第2の暗号化データにより前記第1の暗号化用データに対して暗号化処理を施し、前記第1の暗号化用データから第3の暗号化用データを生成し、この第3の暗号化用データを前記通信手段を介して送信する第1の暗号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記通信手段を介して前記第2及び第3の暗号化用データを受信し、この第2の暗号化用データによりこの第3の暗号化用データに対して復号化処理を施し、この第3の暗号化用データから第1の暗号化用データを生成し提供する第1の復号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記第1の復号化処理手段により生成された前記第1の暗号化用データにより第1の光ディスクデータに対して暗号化処理を施し、この第1の光ディスクデータから第2の光ディスクデータを生成し、この第2の光ディスクデータを前記通信手段を介して前記デコーダ装置側へ提供する第2の暗号化処理手段と、

前記デコーダ装置側に設けられたものであって、前記光ディスクデータを暗号化するための前記第1の暗号化用データと同一の第4の暗号化用データを生成し提供する第4の暗号化用データ生成手段と、

前記デコーダ装置側に設けられたものであって、前記通信手段を介して前記第2の光ディスクデータを受取り、前記第4の暗号化用データによりこの第2の光ディスクデータに対して復号化処理を施し、この第2の光ディスクデータから前記第1の光ディスクデータを生成し提供する第2の復号化処理手段と、

を備えたことを特徴とする光ディスク再生装置。

【請求項8】前記第1の暗号化処理手段が、前記第1の暗号化用データと前記第2の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第3の暗号化用データとして提供する第1の排他的論理和算出手段を有し、

前記第1の復号化処理手段が、前記第2の暗号化用データ

タと前記第 3 の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第 1 の暗号化用データとして提供する第 2 の排他的論理和算出手段を有する、ことを特徴とする請求項 7 に記載の光ディスク再生装置。

【請求項 9】前記第 2 の暗号化用データ生成手段が時間とともに変化する乱数を生成し、この乱数を前記第 2 の暗号化用データとして提供する乱数生成手段を有することを特徴とする請求項 5 又は請求項 7 に記載の光ディスク再生装置。

【請求項 10】前記第 2 の暗号化用データ生成手段における前記第 2 の暗号化用データの生成を制御する制御プログラムを記憶する記憶手段と、前記制御プログラムに基づき前記第 2 の暗号化用データ生成手段における前記第 2 の暗号化用データの生成を制御する制御手段と、を有することを特徴とする請求項 5 又は請求項 7 に記載の光ディスク再生装置。

【請求項 11】光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコード装置と、前記ドライブ装置及び前記デコード装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、

前記光ディスクデータを暗号化するための暗号化用データを生成し提供する暗号化用データ生成手段と、前記通信手段と所定の状態で接続されたものであって、前記暗号化用データを前記通信手段へ出力する出力手段と、前記通信手段と前記所定の状態と同一の状態で接続されたものであって、前記通信手段を介して前記暗号化用データを入力する入力手段と、を備えたことを特徴とする光ディスク記録再生装置。

【請求項 12】光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコード装置と、前記ドライブ装置及び前記デコード装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、

前記ドライブ装置側に設けられたものであって、前記光ディスクデータを暗号化するための第 1 の暗号化用データを生成し提供する第 1 の暗号化用データ生成手段と、

前記ドライブ装置側に設けられ、且つ前記通信手段と所定の状態で接続されたものであって、前記第 1 の暗号化用データを前記通信手段へ出力する出力手段と、前記ドライブ装置側に設けられ、且つ前記通信手段と前記所定の状態と同一の状態で接続されたものであって、前記通信手段を介して前記第 1 の暗号化用データを入力する入力手段と、

前記ドライブ装置側に設けられたものであって、前記入力手段から入力された前記第 1 の暗号化用データにより第 1 の光ディスクデータに対して暗号化処理を施し、この第 1 の光ディスクデータから第 2 の光ディスクデータを生成し、この第 2 の光ディスクデータを前記通信手段を介して前記デコード装置側へ提供する暗号化処理手段と、

前記デコード装置側に設けられたものであって、前記光ディスクデータを暗号化するための前記第 1 の暗号化用データと同一の第 2 の暗号化用データを生成し提供する第 2 の暗号化用データ生成手段と、

前記デコード装置側に設けられたものであって、前記通信手段を介して前記第 2 の光ディスクデータを受取り、前記第 2 の暗号化用データによりこの第 2 の光ディスクデータに対して復号化処理を施し、この第 2 の光ディスクデータから前記第 1 の光ディスクデータを生成し提供する復号化処理手段と、

を備えたことを特徴とする光ディスク記録再生装置。

【請求項 13】光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコード装置と、前記ドライブ装置及び前記デコード装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、

前記光ディスクデータを暗号化するための第 1 の暗号化用データを生成し提供する第 1 の暗号化用データ生成手段と、

前記第 1 の暗号化用データに対して暗号化処理を施し、この第 1 の暗号化用データから第 2 の暗号化用データを生成し、この第 2 の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、

前記通信手段を介して前記第 2 の暗号化用データを受信し、この第 2 の暗号化用データに対して復号化処理を施し、この第 2 の暗号化用データから前記第 1 の暗号化用データを生成し提供する復号化処理手段と、

を備えたことを特徴とする光ディスク記録再生装置。

【請求項 14】光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクから

の反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコード装置と、前記ドライブ装置及び前記デコード装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、

前記ドライブ装置側に設けられたものであって、前記光ディスクデータを暗号化するための第 1 の暗号化用データを生成し提供する第 1 の暗号化用データ生成手段と、前記ドライブ装置側に設けられたものであって、前記第 1 の暗号化用データに対して暗号化処理を施し、この第 1 の暗号化用データから第 2 の暗号化用データを生成し、この第 2 の暗号化用データを前記通信手段を介して送信する第 1 の暗号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記通信手段を介して前記第 2 の暗号化用データを受信し、この第 2 の暗号化用データに対して復号化処理を施し、この第 2 の暗号化用データから前記第 1 の暗号化用データを生成し提供する第 1 の復号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記第 1 の復号化処理手段により生成された前記第 1 の暗号化用データにより第 1 の光ディスクデータに対して暗号化処理を施し、この第 1 の光ディスクデータから第 2 の光ディスクデータを生成し、この第 2 の光ディスクデータを前記通信手段を介して前記デコード装置側へ提供する第 2 の暗号化処理手段と、

前記デコード装置側に設けられたものであって、前記光ディスクデータを暗号化するための前記第 1 の暗号化用データと同一の第 3 の暗号化用データを生成し提供する第 3 の暗号化用データ生成手段と、

前記デコード装置側に設けられたものであって、前記通信手段を介して前記第 2 の光ディスクデータを受取り、前記第 3 の暗号化用データによりこの第 2 の光ディスクデータに対して復号化処理を施し、この第 2 の光ディスクデータから前記第 1 の光ディスクデータを生成し提供する第 2 の復号化処理手段と、

を備えたことを特徴とする光ディスク記録再生装置。

【請求項 15】光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコード装置と、前記ドライブ装置及び前記デコード装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、

前記光ディスクデータを暗号化するための第 1 の暗号化用データを生成し提供する第 1 の暗号化用データ生成手

段と、

前記第 1 の暗号化用データを暗号化するための第 2 の暗号化用データを生成し提供する第 2 の暗号化用データ生成手段と、

前記第 2 の暗号化データにより前記第 1 の暗号化用データに対して暗号化処理を施し、前記第 1 の暗号化用データから第 3 の暗号化用データを生成し、この第 3 の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、

前記通信手段を介して前記第 2 及び第 3 の暗号化用データを受信し、この第 2 の暗号化用データによりこの第 3 の暗号化用データに対して復号化処理を施し、この第 3 の暗号化用データから第 1 の暗号化用データを生成し提供する復号化処理手段と、

を備えたことを特徴とする光ディスク記録再生装置。

【請求項 16】前記暗号化処理手段が、前記第 1 の暗号化用データと前記第 2 の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第 3 の暗号化用データとして提供する第 1 の排他的論理和算出手段を有し、

前記復号化処理手段が、前記第 2 の暗号化用データと前記第 3 の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第 1 の暗号化用データとして提供する第 2 の排他的論理和算出手段を有する、

ことを特徴とする請求項 15 に記載の光ディスク記録再生装置。

【請求項 17】光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコード装置と、前記ドライブ装置及び前記デコード装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、

前記ドライブ装置側に設けられたものであって、前記光ディスクデータを暗号化するための第 1 の暗号化用データを生成し提供する第 1 の暗号化用データ生成手段と、

前記ドライブ装置側に設けられたものであって、前記第 1 の暗号化用データを暗号化するための第 2 の暗号化用データを生成し提供する第 2 の暗号化用データ生成手段と、

前記ドライブ装置側に設けられたものであって、前記第 2 の暗号化データにより前記第 1 の暗号化用データに対して暗号化処理を施し、前記第 1 の暗号化用データから第 3 の暗号化用データを生成し、この第 3 の暗号化用データを前記通信手段を介して送信する第 1 の暗号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記通

信手段を介して前記第2及び第3の暗号化用データを受信し、この第2の暗号化用データによりこの第3の暗号化用データに対して復号化処理を施し、この第3の暗号化用データから第1の暗号化用データを生成し提供する第1の復号化処理手段と、

前記ドライブ装置側に設けられたものであって、前記第1の復号化処理手段により生成された前記第1の暗号化用データにより第1の光ディスクデータに対して暗号化処理を施し、この第1の光ディスクデータから第2の光ディスクデータを生成し、この第2の光ディスクデータを前記通信手段を介して前記デコーダ装置側へ提供する第2の暗号化処理手段と、

前記デコーダ装置側に設けられたものであって、前記光ディスクデータを暗号化するための前記第1の暗号化用データと同一の第4の暗号化用データを生成し提供する第4の暗号化用データ生成手段と、

前記デコーダ装置側に設けられたものであって、前記通信手段を介して前記第2の光ディスクデータを受取り、前記第4の暗号化用データによりこの第2の光ディスクデータに対して復号化処理を施し、この第2の光ディスクデータから前記第1の光ディスクデータを生成し提供する第2の復号化処理手段と、

を備えたことを特徴とする光ディスク記録再生装置。

【請求項18】前記第1の暗号化処理手段が、前記第1の暗号化用データと前記第2の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第3の暗号化用データとして提供する第1の排他的論理和算出手段を有し、

前記第1の復号化処理手段が、前記第2の暗号化用データと前記第3の暗号化用データとの排他的論理和を算出し、この排他的論理和の値を前記第1の暗号化用データとして提供する第2の排他的論理和算出手段を有する、ことを特徴とする請求項17に記載の光ディスク記録再生装置。

【請求項19】前記第2の暗号化用データ生成手段が時間とともに変化する乱数を生成し、この乱数を前記第2の暗号化用データとして提供する乱数生成手段を有することを特徴とする請求項15又は請求項17に記載の光ディスク記録再生装置。

【請求項20】前記第2の暗号化用データ生成手段における前記第2の暗号化用データの生成を制御する制御プログラムを記憶する記憶手段と、

前記制御プログラムに基づき前記第2の暗号化用データ生成手段における前記第2の暗号化用データの生成を制御する制御手段と、

を有することを特徴とする請求項15又は請求項17に記載の光ディスク記録再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、光ディスクに記

録されている光ディスクデータを再生する光ディスク再生装置、及び光ディスクに記録されている光ディスクデータの再生並びに光ディスクに対するデータの記録を行う光ディスク記録再生装置に関する。特に、光ディスクデータの不正コピーを防止するため、必要に応じて光ディスクデータを暗号化する光ディスク再生装置、及び光ディスク記録再生装置に関する。

【0002】

【従来の技術】近年、大容量情報記憶媒体としてDVD(Digital Video Disk)-ROM及びDVD-RAM等の光ディスクが注目をあびている。前者は再生専用の情報記憶媒体であり、後者は書換え可能な情報記録媒体である。

【0003】ここで、このような光ディスクに記録されている光ディスクデータを再生する光ディスク再生装置、及びこのような光ディスクに記録されている光ディスクデータの再生並びに光ディスクに対するデータの記録を行う光ディスク記録再生装置について簡単に説明する。なお、ここでは、光ディスク再生装置及び光ディスク記録再生装置の両者を併せて光ディスク装置と称する。

【0004】光ディスク装置は、例えば、ドライブ装置、デコーダ装置(パーソナルコンピュータなど)、及びバスライン等より構成されている。ドライブ装置は、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するものである。デコーダ装置は、ドライブ装置から提供される光ディスクデータを再生するものである。バスラインは、ドライブ装置及びデコーダ装置間のデータ通信、並びにドライブ装置内及びデコーダ装置内のデータ通信を担うものである。

【0005】また、ドライブ装置には、第1のバスキー生成部及び暗号化処理部が設けられている。第1のバスキー生成部ではバスキーなるものが生成される。この第1のバスキー生成部で生成されたバスキーは、バスラインを介して暗号化処理部へ送信される。暗号化処理部では、送信されたバスキーにより光ディスクデータに対して暗号化処理が施される。

【0006】デコーダ装置には、第2のバスキー生成部及び復号化処理部が設けられている。第2のバスキー生成部では、第1のバスキー生成部で生成されるバスキーと同一のバスキーが生成される。この第2のバスキー生成部で生成されたバスキーは、復号化処理部へ送信される。復号化処理部では、送信されたバスキーにより暗号化された光ディスクデータに対して復号化処理が施される。

【0007】ドライブ装置側からデコーダ装置側へバスラインを介して光ディスクデータを送信する場合、光ディスクデータはドライブ装置側(第1のバスキー生成部)で生成されたバスキーにより暗号化されてから送信



される。つまり、デコーダ装置側では、暗号化された光ディスクデータが受信される。そして、デコーダ装置側では、このデコーダ装置側（第2のバスキー生成部）で生成されたバスキーにより暗号化された光ディスクデータが復号化される。

【0008】このように、バスラインを介して送信される光ディスクデータを暗号化することにより、バスライン上における光ディスクデータのセキュリティが確保されている。具体的に説明すると、光ディスクデータを不正にコピーしようとする者が、バスラインから光ディスクデータを読み出したとしても、読み出された光ディスクデータは暗号化されているため、この者の目的は達成されないというものである。

【0009】

【発明が解決しようとする課題】ところが、このような光ディスク装置の場合、バスライン上のデータが解析されることにより、バスキーが解読されてしまい、その結果、光ディスクデータが不正にコピーされてしまうという問題点があった。

【0010】つまり、バスキーが解読されてしまうと、バスキーにより暗号化された光ディスクデータは、暗号化されていないもの同然となってしまう。よって、光ディスクデータが不正にコピーされてしまうということになる。

【0011】この発明の目的は、上記したような事情に鑑み成されたものであって、光ディスクデータの不正コピーを防止することが可能な光ディスク再生装置及び光ディスク記録再生装置を提供することにある。

【0012】

【課題を解決するための手段】上記課題を解決し目的を達成するために、この発明の光ディスク再生装置及び光ディスク記録再生装置は、以下のように構成されている。

(1) この発明は、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、前記光ディスクデータを暗号化するための暗号化用データを生成し提供する暗号化用データ生成手段と、前記通信手段と所定の状態で接続されたものであって、前記暗号化用データを前記通信手段へ出力する出力手段と、前記通信手段と前記所定の状態と同一の状態で接続されたものであって、前記通信手段を介して前記暗号化用データを入力する入力手段とを備えている。

【0013】(2) この発明は、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、こ

この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、前記光ディスクデータを暗号化するための第1の暗号化用データを生成し提供する第1の暗号化用データ生成手段と、前記第1の暗号化用データに対して暗号化処理を施し、この第1の暗号化用データから第2の暗号化用データを生成し、この第2の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、前記通信手段を介して前記第2の暗号化用データを受信し、この第2の暗号化用データに対して復号化処理を施し、この第2の暗号化用データから前記第1の暗号化用データを生成し提供する復号化処理手段とを備えている。

【0014】(3) この発明は、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク再生装置において、前記光ディスクデータを暗号化するための第1の暗号化用データを生成し提供する第1の暗号化用データ生成手段と、前記第1の暗号化用データを暗号化するための第2の暗号化用データを生成し提供する第2の暗号化用データ生成手段と、前記第2の暗号化データにより前記第1の暗号化用データに対して暗号化処理を施し、前記第1の暗号化用データから第3の暗号化用データを生成し、この第3の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、前記通信手段を介して前記第2及び第3の暗号化用データを受信し、この第2の暗号化用データによりこの第3の暗号化用データに対して復号化処理を施し、この第3の暗号化用データから第1の暗号化用データを生成し提供する復号化処理手段とを備えている。

【0015】(4) この発明は、光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、前記光ディスクデータを暗号化するための暗号化用データを生成し提供する暗号化用データ生成手段と、前記通信手段と所定の状態で接続されたものであって、前記暗号化用データを前記通信

手段へ出力する出力手段と、前記通信手段と前記所定の状態と同一の状態とで接続されたものであって、前記通信手段を介して前記暗号化用データを入力する入力手段とを備えている。

【0016】(5) この発明は、光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、前記光ディスクデータを暗号化するための第1の暗号化用データを生成し提供する第1の暗号化用データ生成手段と、前記第1の暗号化用データに対して暗号化処理を施し、この第1の暗号化用データから第2の暗号化用データを生成し、この第2の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、前記通信手段を介して前記第2の暗号化用データを受信し、この第2の暗号化用データに対して復号化処理を施し、この第2の暗号化用データから前記第1の暗号化用データを生成し提供する復号化処理手段とを備えている。

【0017】(6) この発明は、光ディスクに対して光ビームを照射し、光ディスクに対して所定のデータを記録するとともに、光ディスクに対して光ビームを照射し、光ディスクからの反射光を受光し、この受光された反射光に反映された光ディスクデータを提供するドライブ装置と、このドライブ装置から提供される光ディスクデータを再生するデコーダ装置と、前記ドライブ装置及び前記デコーダ装置の間のデータ通信、並びにこのドライブ装置内のデータ通信を担う通信手段とを備えた光ディスク記録再生装置において、前記光ディスクデータを暗号化するための第1の暗号化用データを生成し提供する第1の暗号化用データ生成手段と、前記第1の暗号化用データを暗号化するための第2の暗号化用データを生成し提供する第2の暗号化用データ生成手段と、前記第2の暗号化用データにより前記第1の暗号化用データに対して暗号化処理を施し、前記第1の暗号化用データから第3の暗号化用データを生成し、この第3の暗号化用データを前記通信手段を介して送信する暗号化処理手段と、前記通信手段を介して前記第2及び第3の暗号化用データを受信し、この第2の暗号化用データによりこの第3の暗号化用データに対して復号化処理を施し、この第3の暗号化用データから第1の暗号化用データを生成し提供する復号化処理手段とを備えている。

【0018】上記手段を講じた結果、光ディスクデータを暗号化するためのデータが、暗号化された上で通信手段を介して送信される。これにより、光ディスクデータ

を暗号化するためのデータの解析を困難なものとすることが可能となる。

【0019】

【発明の実施の形態】以下、この発明の実施の形態について図面を参照して説明する。図1は、この発明の一実施の形態に係る光ディスク装置（光ディスク再生装置及び光ディスク記録再生装置）の概略構成を示す図である。

【0020】図1に示すように、光ディスク装置1は、ドライブ装置100、デコーダ装置200、通信手段としてのバスライン300等により構成されている。ドライブ装置100には、ドライブ制御部101、メモリ102、デコーダ認証処理部103、レーザ駆動制御部104、光ピックアップ部105、アナログ信号処理部106、サーボ制御部107、DVD信号処理部108、DRAM109、CD（Compact Disc）信号処理部110、DRAM111等が設けられている。

【0021】また、光ピックアップ部105には、半導体レーザ105a、及び光検出器105b等が設けられている。さらに、光ディスク装置1が光ディスク記録再生装置の場合には、ドライブ装置100には、記録用データ処理部112が設けられている。なお、上記したドライブ制御部101、メモリ102、デコーダ認証処理部103、DVD信号処理部108、及び記録用データ処理部112は、バスライン300に接続されている。

【0022】ドライブ制御部101は、メモリ102に記憶されたドライブ制御プログラムに基づきドライブ装置100全体を制御するものである。デコーダ認証処理部103は、後述する相互認証処理によりデコーダ装置を認証するものである。レーザ駆動制御部104は、半導体レーザ105aを制御するものであり、この光ディスク装置が光ディスク再生装置の場合と光ビーム記録再生装置の場合とで機能が異なる。この光ディスク装置が光ディスク再生装置の場合には、レーザ駆動制御部104は、光ディスクに記録されたデータを再生するための再生用光ビームを半導体レーザ105aから照射させる。この光ディスク装置が光ディスク記録再生装置の場合には、レーザ駆動制御部104は、光ディスクに記録されたデータを再生するための再生用光ビーム及び光ディスクにデータを記録するための記録用光ビームを照射させる。なお、レーザ駆動制御部104は、半導体レーザ105から記録用光ビームを照射させる際、記録用データ処理部114から提供される記録用データに基づき半導体レーザを制御する。

【0023】光ピックアップ部105に設けられた光検出器105bは、半導体レーザ105aから照射された再生用光ビームの光ディスクからの反射光を受光するものである。アナログ信号処理部106は、光検出器105bにより検出された光ディスクからの反射光を処理するものである。簡単に説明すると、反射光に反映された



光ディスクデータからDVD信号とCD信号とを区別し、DVD信号をサーボ制御部107及びDVD信号処理部108へ提供し、CD信号をCD信号処理部110へ提供する。サーボ制御部107は、アナログ信号処理部106から提供されるDVD信号に基づき、フォーカス制御、トラッキング制御、及びリニアモータ制御を行うものである。DVD信号処理部108は、アナログ信号処理部106から提供されるDVD信号に対して各種処理を施すものであり、このDVD信号処理部108については後に詳しく説明する。DRAM109は、例えば、4Mバイトの容量を有し、バッファとして機能する。CD信号処理部110は、アナログ信号処理部106から提供されるCD信号に対して各種処理を施すものである。DRAM111は、例えば128Kバイトの容量を有し、バッファとして機能する。

【0024】デコーダ装置200には、デコーダ制御部201、メモリ202、及びドライブ認証処理部203等が設けられている。また、これら、デコーダ制御部201、メモリ202、及びドライブ認証処理部203は、バスライン300に接続されている。

【0025】デコーダ制御部201は、メモリ202に記憶されたデコーダ制御プログラムに基づきデコーダ装置200全体を制御するものである。ドライブ認証処理部203は、後述する相互認証処理によりドライブ装置を認証するものである。

【0026】続いて、DVD-ROM及びDVD-RAMのデータ構造について簡単に説明する。DVD-ROM及びDVD-RAMには、リードインエリア、データエリア、及びリードアウトエリアなどがフォーマットされている。これらエリアは、複数のゾーンで構成されており、各ゾーンは複数のトラックにより構成されている。また、リードインエリア内には、CPR\_MAI (Copyright Management Information) フィールド及びメインデータフィールドがフォーマットされている。同様に、データエリア内にも、CPR\_MAIフィールド及びメインデータフィールドがフォーマットされている。

【0027】リードインエリア内のCPR\_MAI (Copyright Management Information) フィールドには、認証コード (Authentication Control code) が記録されている。この認証コードは、ドライブ装置100とデコーダ装置200との相互認証の計算を行う際に用いられる5ビットのデータである。

【0028】データエリア内のCPR\_MAIフィールドには、タイトルキー (Encrypted Title Key) が記録されている。このタイトルキーは、1枚の光ディスクの中に複数のタイトルが格納されている場合、これらタイトル夫々を暗号化する5バイトの鍵データである。

【0029】リードインエリア内のメインデータフィールドには、ディスクキー (Secured Disk Key Data) が

記録されている。このディスクキーは、1枚のディスクの中に複数のタイトルが格納されている場合、これらタイトルをディスク全体にわたって暗号化する2048バイトの共通の鍵データである。

【0030】データエリア内のメインデータフィールドには、スクランブルAVデータが記録されている。このスクランブルAVデータは、図示しないスクランブラ (ブラックボックス) 及びタイトルキーによりスクランブルされたAVデータである。

10 【0031】続いて、ドライブ装置100とデコーダ装置200との間で行われる相互認証処理について説明する。ドライブ装置100側には、既に説明したようにデコーダ装置200を認証するためのデコーダ認証部103が設けられている。同様に、デコーダ装置200側にも、ドライブ装置100を認証するためのドライブ認証部203が設けられている。相互認証処理は、CPR\_MAIフィールドに記録されている認証コードを利用して進められる。ここで、認証コードを利用して進められる相互認証処理について具体的に説明する。

20 【0032】はじめに、デコーダ装置200のドライブ認証処理部203において、乱数を用いた80ビットのチャレンジデータ1が生成される。このチャレンジデータ1は、デコーダ装置200側からドライブ装置100側へ送信され、ドライブ装置100のデコーダ認証処理部103へ入力される。このデコーダ認証処理部103では、光ディスクから読出された認証コード及びチャレンジデータ1から40ビットのレスポンスデータ1が計算される。このレスポンスデータ1は、ドライブ装置100側からデコーダ装置200側へ送信され、デコーダ装置200のドライブ認証処理部203へ入力される。このドライブ認証処理部203では、チャレンジデータ1から計算された結果 (40ビットデータ) とレスポンスデータ1とを比較して、これらが等しいとき、ドライブ装置100が認証される。

30 【0033】次に、ドライブ装置100のデコーダ認証処理部103において、乱数を用いた80ビットのチャレンジデータ2が生成される。このチャレンジデータ2は、ドライブ装置100側からデコーダ装置200側へ送信され、デコーダ装置200のドライブ認証処理部203へ入力される。このドライブ認証処理部203では、チャレンジデータ2から40ビットのレスポンスデータ2が計算される。このレスポンスデータ2は、デコーダ装置200側からドライブ装置100側へ送信され、ドライブ装置100のデコーダ認証処理部103へ入力される。このデコーダ認証処理部103では、チャレンジデータ2及び認証コードから計算された結果とレスポンスデータ2とを比較して、これらが等しいとき、デコーダ装置200が認証される。

40 【0034】デコーダ装置200側でドライブ装置100が認証され、ドライブ装置100側でデコーダ装置2

00が認証されることにより、相互認証処理が完了する。続いて、デコーダ認証処理部103側で生成されたバスキーをバスライン300を介してデコーダ認証処理部103側からDVD信号処理部108側へ送信し、このバスキーにより暗号化されたディスクキー及びタイトルキー（以下鍵束データと称する）をバスライン300を介してドライブ装置100側からデコーダ装置200側へ送信する処理について説明する。

【0035】まず、バスキーの送信処理その1について説明する。図2は、バスキーの送信処理その1を実現するための構成を示す図である。バスキーにより暗号化される鍵束データは、光ディスクから読取られ、DVD信号処理回路108を経由して、DRAM109に書込まれる。

【0036】図2に示すように、デコーダ認証処理部103には、暗号化用データ生成手段としての第1のバスキー生成部103a、及び出力手段としてのバスキー出力部103bが設けられている。第1のバスキー生成部103aは、上記説明した相互認証処理によりドライブ装置及びデコーダ装置が相互に認証されることを条件として、第1のバスキーを生成するものである。この第1のバスキーは、鍵束データの暗号化に利用されるものである。バスキー出力部103bは、第1のバスキーをバスライン300へ出力するものである。このバスキー出力部103bは、バスライン300と図2に示すような特定の状態で接続するように構成されているものとする。つまり、このバスキー出力部103bから出力される第1のバスキーは、バスキー出力部103bがバスライン300と特定の状態で接続されることにより、暗号化されてバスライン300上へ出力されることになる。

【0037】DVD信号処理部108には、暗号化処理手段としての鍵束データ暗号化処理部108a、及び入力手段としてのバスキー入力部108bが設けられている。バスキー入力部108bは、バスキー出力部103bから出力された第1のバスキーをバスライン300を介してDVD信号処理部108へ入力するものである。このバスキー入力部108bは、バスライン300と図2に示すような特定の状態で接続するように構成されているものとする。つまり、バスキー出力部103bから出力された第1のバスキーが、このバスキー入力部108bを介して入力されることにより復号化されることになる。鍵束データ暗号化処理部108aは、DRAM109から読出された鍵束データに対してバスキー入力部108bを介して得られた第1のバスキーにより暗号化処理を施し、暗号化処理済鍵束データを提供する。具体的に説明すると、鍵束データ暗号化処理部108aは、鍵束データと第1のバスキーとの排他的論理和を算出する。つまり、ここで算出された排他的論理和の値が暗号化処理済鍵束データということになる。鍵束データ暗号化処理部108aから提供される暗号化処理済鍵束デ

タは、バスライン300を介してデコーダ装置200側へ送信される。

【0038】ドライブ認証処理部203には、暗号化用データ生成手段としての第2のバスキー生成部203a、及び復号化処理手段としての鍵束データ復号化処理部203bが設けられている。第2のバスキー生成部203aは、上記説明した相互認証処理によりドライブ装置及びデコーダ装置が相互に認証されことを条件として、第1のバスキーと同一のデータである第2のバスキーを生成する。この第2のバスキーは、第1のバスキーにより暗号化された暗号化処理済鍵束データの復号化に利用されるものである。鍵束データ復号化処理部203bは、第1のバスキーにより暗号化された暗号化処理済鍵束データに対して、第2のバスキーにより復号化処理を施し、元の鍵束データと同一の復号化処理済鍵束データを提供するものである。

【0039】以上説明した鍵束データの送信処理その1によれば、デコーダ認証処理部103からDVD信号処理部108へ送信される第1のバスキーを暗号化することにより、バスライン300上のデータが解析されることによる第1のバスキーの解読を防止することができる。つまり、第1のバスキーが解読されなければ、この第1のバスキーにより暗号化された鍵束データが解析されるのを防止することができ、結果的に、光ディスクデータの不正コピーが防止できる。

【0040】次に、鍵束データの送信処理その2について説明する。図3は、鍵束データの送信処理その2を実現するための構成を示す図である。図3に示すように、デコーダ認証処理部103には、暗号化用データ生成手段としての第1のバスキー生成部103a、及び暗号化処理手段としてのバスキー暗号化処理部103cが設けられている。第1のバスキー生成部103aは、上記説明した相互認証処理によりドライブ装置及びデコーダ装置が相互に認証されことを条件として、第1のバスキーを生成するものである。この第1のバスキーは、鍵束データの暗号化に利用されるものである。バスキー暗号化処理部103cは、第1のバスキーを暗号化して暗号化された暗号化処理済バスキーをバスライン300へ出力するものである。

【0041】ここで、バスキー暗号化処理部103cにおける暗号化処理について説明する。バスキー暗号化処理部103cには、乱数生成手段としての疑似雑音発生回路103d、及び第1の排他的論理和算出手段としての排他的論理和算出回路103eが設けられている。疑似雑音発生回路103dは、nビットの乱数を発生させるものである。乱数は、固定されたものであってもよいし、時間とともに変化するものであってもよい。排他的論理和算出回路103eは、第1のバスキーと乱数との排他的論理和を算出するものである。また、この排他的論理和の値が暗号化処理済バスキーとして、バスラ

イン300を介してDVD信号処理部108へ送信される。

【0042】DVD信号処理部108には、暗号化処理手段としての鍵束データ暗号化処理部108a、及び復号化処理手段としてのバスキー復号化処理部108cが設けられている。バスキー復号化処理部108cは、バスライン300を介して送信される暗号化処理済バスキーに対して復号化処理を施し、第1のバスキーと同一の復号化処理済バスキーを提供するものである。ここで、バスキー復号化処理部108cにおける復号化処理について説明する。バスキー復号化処理108cには、乱数入力部108d、及び第2の排他的論理和算出手段としての排他的論理和算出回路108eが設けられている。乱数入力部108dは、疑似雑音発生回路103dで発生された乱数をバスライン300を介して受取るものである。排他的論理和算出回路108eは、バスライン300を介して送信される暗号化処理済バスキーと乱数入力部108dで受取られた乱数との排他的論理和を算出するものである。また、この排他的論理和の値が第1のバスキーと同一の復号化処理済バスキーとして提供される。

【0043】鍵束データ暗号化処理部108aは、DRAM109から読出される鍵束データに対してバスキー復号化処理部108cから提供される第1のバスキーにより暗号化処理を施し、暗号化処理済鍵束データを提供する。具体的に説明すると、鍵束データ暗号化処理部108aは、鍵束データと第1のバスキーとの排他的論理和を算出する。つまり、ここで算出された排他的論理和の値が暗号化処理済鍵束データということになる。鍵束データ暗号化処理部108aから提供される暗号化処理済鍵束データは、バスライン300を介してデコーダ装置200側へ送信される。

【0044】ドライブ認証処理部203には、暗号化用データ生成手段としての第2のバスキー生成部203a、及び復号化処理手段としての鍵束データ復号化処理部203bが設けられている。第2のバスキー生成部203aは、上記説明した相互認証処理によりドライブ装置及びデコーダ装置が相互に認証されことを条件として、第1のバスキーと同一のデータである第2のバスキーを生成するものである。この第2のバスキーは、第1のバスキーにより暗号化された暗号化処理済鍵束データの復号化に利用されるものである。鍵束データ復号化処理部203bは、第1のバスキーにより暗号化された暗号化処理済鍵束データに対して、第2のバスキーにより復号化処理を施し、元の鍵束データと同一の復号化処理済鍵束データを提供するものである。

【0045】以上説明した鍵束データの送信処理その2によれば、デコーダ認証処理部103からDVD信号処理部108へ送信される第1のバスキーを暗号化することにより、バスライン300上のデータ解析による第1

のバスキーの解読を防止することができる。つまり、第1のバスキーが解読されなければ、この第1のバスキーにより暗号化された鍵束データが解析されるのを防止することができ、結果的に、光ディスクデータの不正コピーが防止できる。

【0046】次に、鍵束データの送信処理その3について説明する。図3は、鍵束データの送信処理その3を実現するための構成を示す図である。図3に示すように、デコーダ認証処理部103には、暗号化用データ生成手段としての第1のバスキー生成部103a、及び暗号化処理手段としてのバスキー暗号化処理部103fが設けられている。第1のバスキー生成部103aは、上記説明した相互認証処理によりドライブ装置及びデコーダ装置が相互に認証されことを条件として、第1のバスキーを生成する。この第1のバスキーは、鍵束データの暗号化に利用されるものである。バスキー暗号化処理部103fは、第1のバスキーを暗号化して暗号化された暗号化処理済バスキーをバスライン300へ出力するものである。

【0047】ここで、バスキー暗号化処理部103fにおける暗号化処理について説明する。バスキー暗号化処理部103fには、暗号化用データ生成手段としてのレジスタ103g、及び第1の排他的論理和算出手段としての排他的論理和算出回路103hが設けられている。レジスタ103gは、nビットのデータを出力するものである。また、このレジスタ103gから出力されるnビットのデータは、記憶手段としてのメモリ102に記憶されたプログラムに基づき生成されるものとする。このとき、プログラムに基づくnビットのデータ生成は、制御手段としてのドライブ制御部101により行われるものとする。排他的論理和算出回路103hは、第1のバスキーとnビットのデータとの排他的論理和を算出するものである。また、この排他的論理和の値が暗号化処理済バスキーとして、バスライン300を介してDVD信号処理部108へ送信される。

【0048】DVD信号処理部108には、暗号化処理手段としての鍵束データ暗号化処理部108a、及び復号化処理手段としてのバスキー復号化処理部108fが設けられている。バスキー復号化処理部108fは、バスライン300を介して送信される暗号化処理済バスキーに対して復号化処理を施し、第1のバスキーと同一の復号化処理済バスキーを提供するものである。ここで、バスキー復号化処理部108fにおける復号化処理について説明する。バスキー復号化処理108fには、レジスタ108g、及び第2の排他的論理和算出手段としての排他的論理和算出回路108hが設けられている。レジスタ108gは、nビットのデータを出力するものである。また、このレジスタ108gから出力されるnビットのデータは、記憶手段としてのメモリ102に記憶されたプログラムに基づき生成されるものとする。この

とき、プログラムに基づくnビットのデータ生成は、制御手段としてのドライブ制御部101により行われるものとする。従って、レジスタ103gから出力されるデータと、レジスタ108gから出力されるデータとは同一のデータとなる。

【0049】排他的論理和算出回路108hは、バスライン300を介して送信される暗号化処理済バスキーとレジスタ108gから出力されるnビットのデータとの排他的論理和を算出するものである。また、この排他的論理和の値が第1のバスキーと同一の復号化処理済バス

キーとして提供される。  
【0050】鍵束データ暗号化処理部108aは、DRAM109から読出される鍵束データに対してバスキー復号化処理部108cから提供される第1のバスキーにより暗号化処理を施し、暗号化処理済鍵束データを提供する。具体的に説明すると、鍵束データ暗号化処理部108aは、鍵束データと第1のバスキーとの排他的論理和を算出する。つまり、ここで算出された排他的論理和の値が暗号化処理済鍵束データということになる。鍵束データ暗号化処理部108aから提供される暗号化処理済鍵束データは、バスライン300を介してデコーダ装置200側へ送信される。

【0051】ドライブ認証処理部203には、第2のバスキー生成部203a、及び鍵束データ復号化処理部203bが設けられている。第2のバスキー生成部203aは、上記説明した相互認証処理によりドライブ装置及びデコーダ装置が相互に認証されことを条件として、第1のバスキーと同一のデータである第2のバスキーを生成するものである。この第2のバスキーは、第1のバスキーにより暗号化された暗号化処理済鍵束データの復号化に利用されるものである。鍵束データ復号化処理部203bは、第1のバスキーにより暗号化された暗号化処理済鍵束データに対して、第2のバスキーにより復号化処理を施し、元の鍵束データと同一の復号化処理済鍵束データを提供するものである。

【0052】以上説明した鍵束データの送信処理その3によれば、デコーダ認証処理部103からDVD信号処理部108へ送信される第1のバスキーを暗号化することにより、バスライン300上のデータ解析による第1のバスキーの解読を防止することができる。つまり、第1のバスキーが解読されなければ、この第1のバスキーにより暗号化された鍵束データが解析されるのを防止することができ、結果的に、光ディスクデータの不正コピーが防止できる。

【0053】

【発明の効果】この発明によれば、光ディスクデータの不正コピーを防止することが可能な光ディスク再生装置及び光ディスク記録再生装置を提供できる。

【図面の簡単な説明】

【図1】この発明の一実施の形態に係る光ディスク装置（光ディスク再生装置及び光ディスク記録再生装置）の概略構成を示す図である。

【図2】バスキーの送信処理その1を実現するための構成を示す図である。

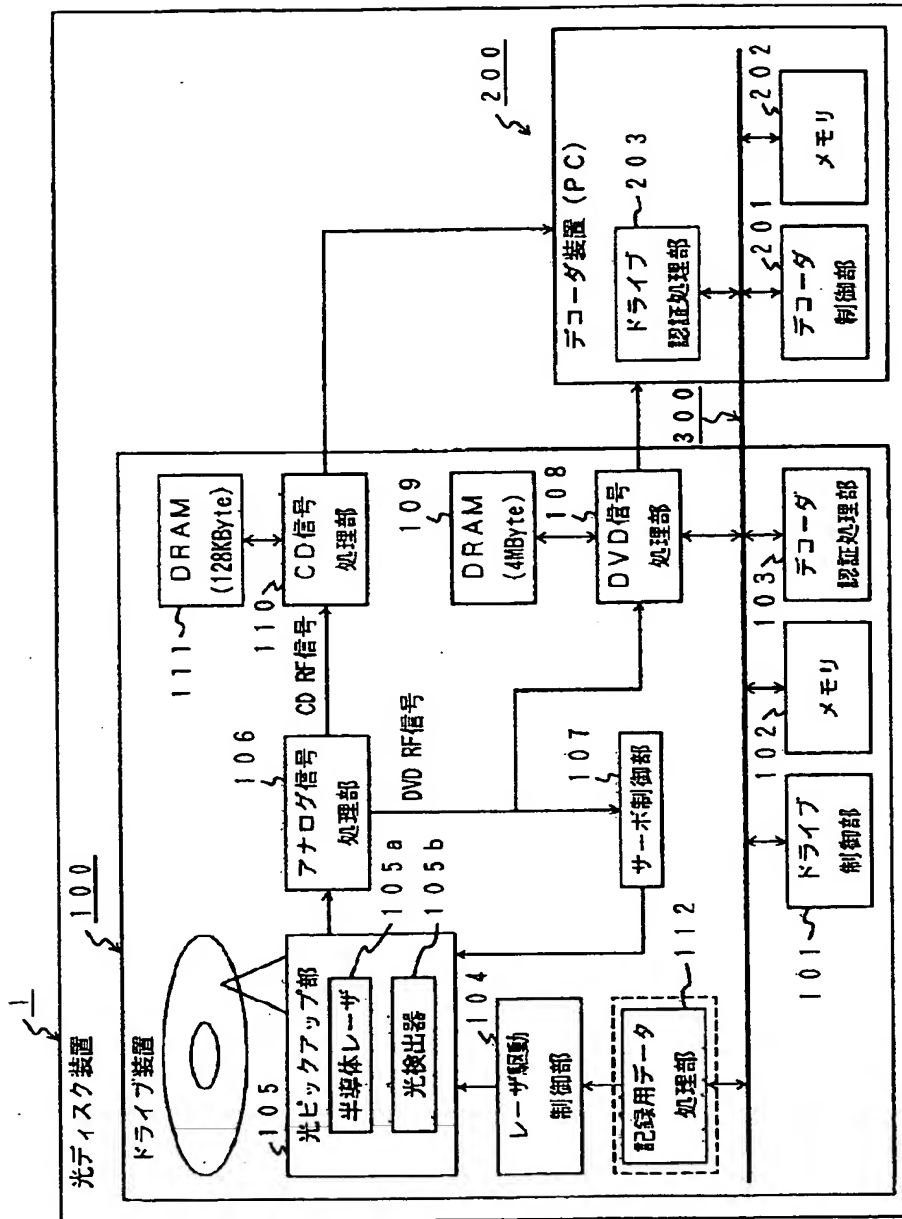
【図3】バスキーの送信処理その2を実現するための構成を示す図である。

【図4】バスキーの送信処理その3を実現するための構成を示す図である。

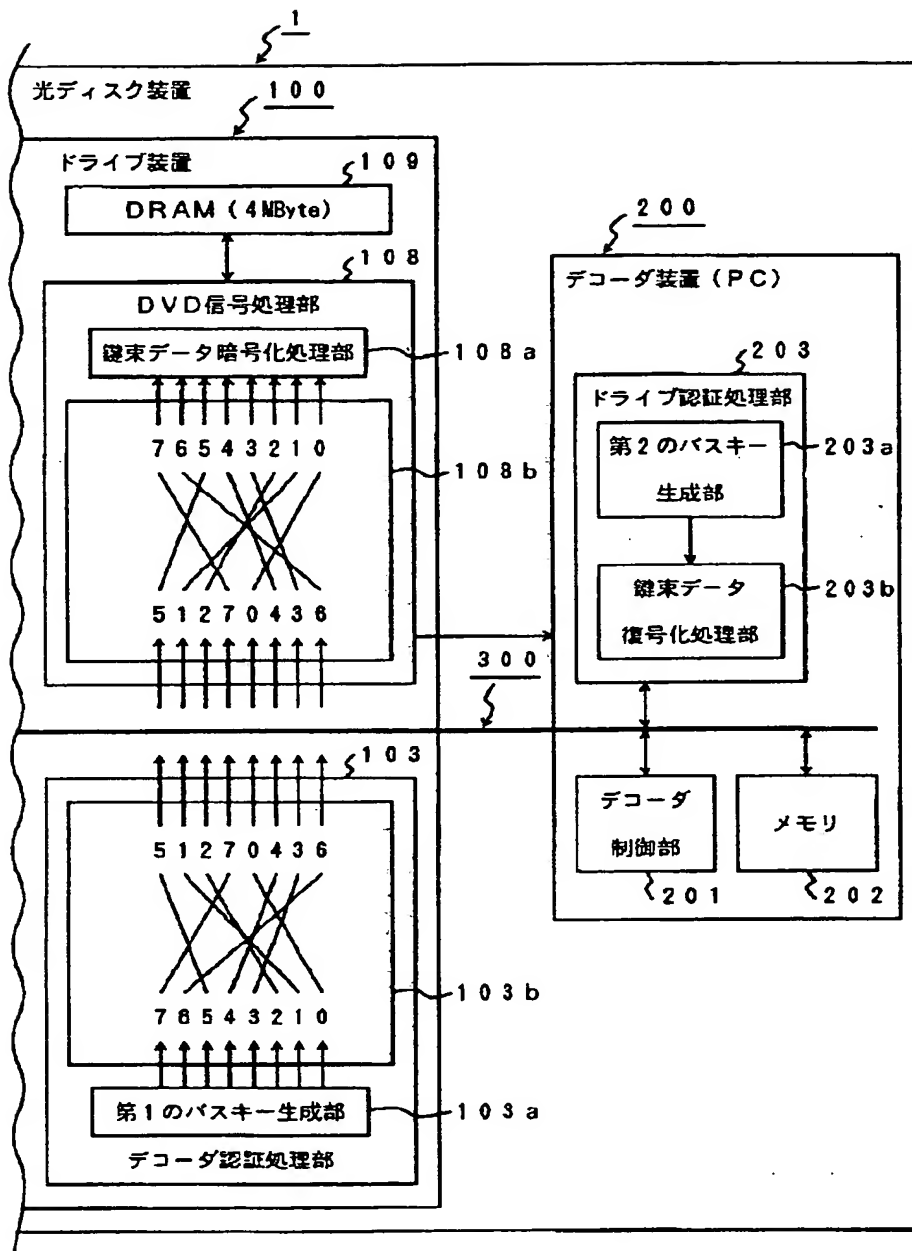
【符号の説明】

- 1…光ディスク装置
- 100…ドライブ装置
- 101…ドライブ制御部
- 102…メモリ
- 103…デコーダ認証処理部
- 108…DVD信号処理部
- 200…デコーダ装置
- 201…デコーダ制御部
- 202…メモリ
- 203…ドライブ認証処理部
- 300…バスライン

【図1】

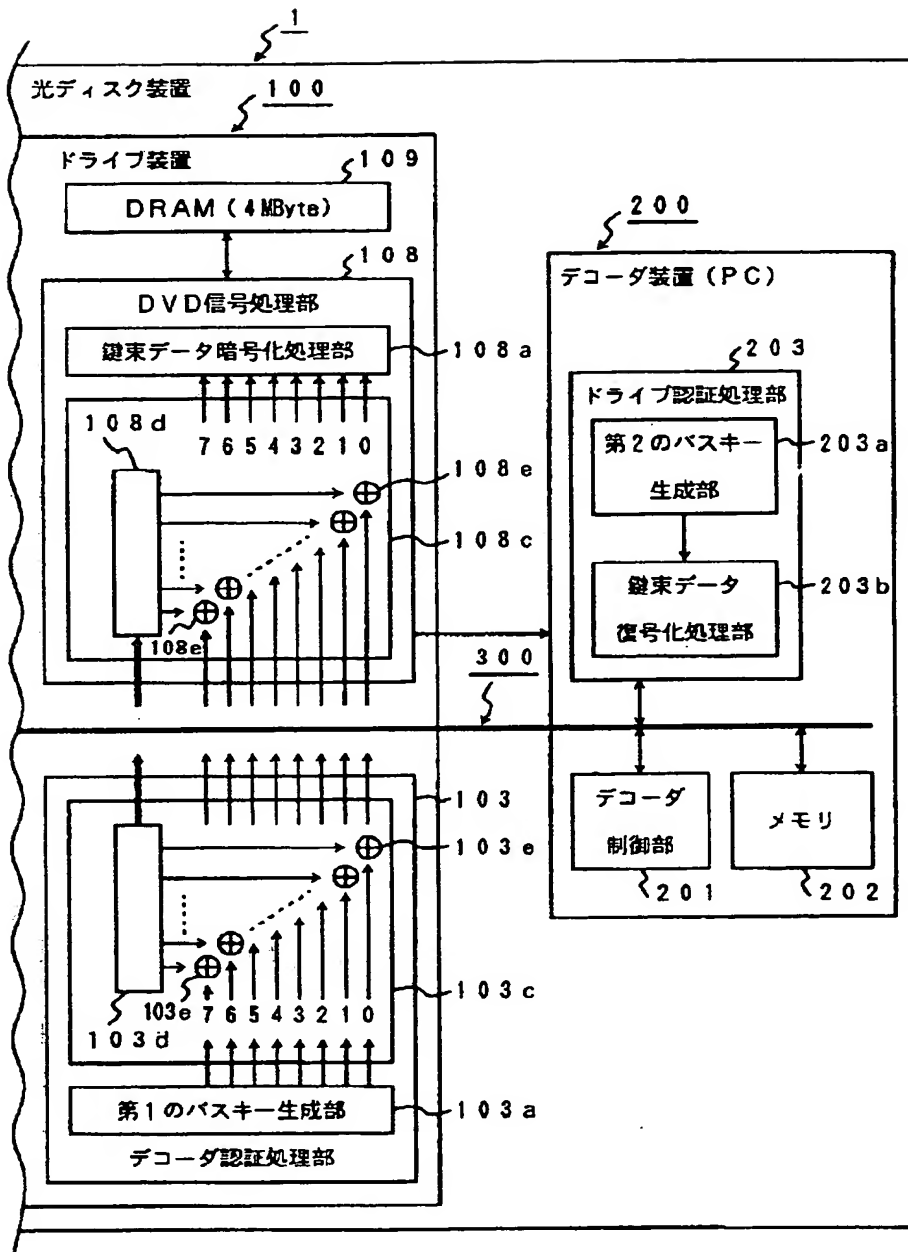


【図2】

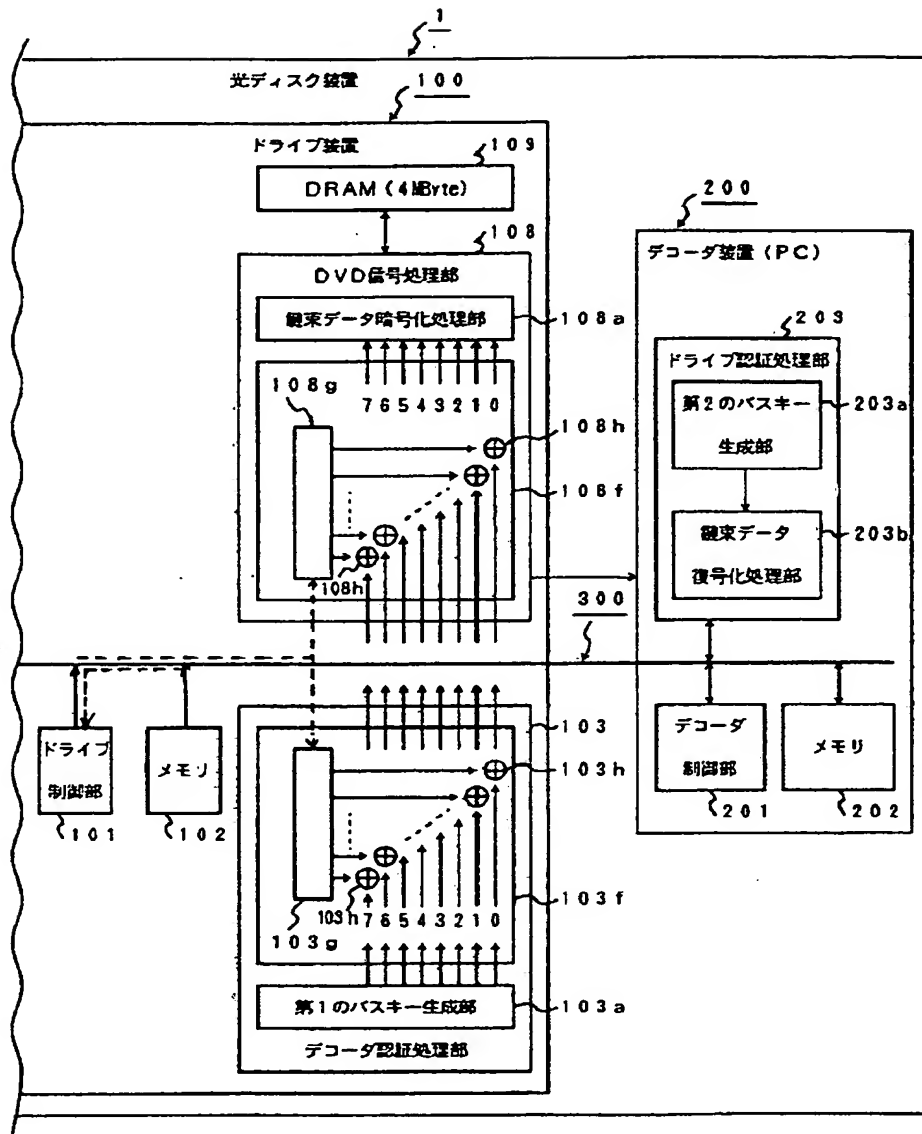




【図3】



【図4】



フロントページの続き

(51)Int.Cl.<sup>9</sup>

G11B 20/18

識別記号

542

F1

G11B 20/18

542Z